**Step by step guide to security**

### External Relations
1. Complete a vulnerabilities assessment
2. Determine what external influences increase your vulnerability
3. Identify decision makers
4. Lobby for change at all levels

### Professional Security Staff
1. Communicate organisational expectations
2. Recruit professional staff and undertake a formal induction
3. Develop organisational procedures
4. Develop facility-specific site orders
5. Implement training programs
6. Develop a Security Management Plan

### Electronic Security
1. Document specifications
2. Communicate expectations and objectives
3. Audit existing equipment
4. Seek professional advice

### Physical Security
1. Document specifications
2. Communicate expectations and objectives
3. Audit existing equipment
4. Seek professional advice

### Incident and Emergency Management
1. Establish an Emergency Planning Committee
2. Complete a threat assessment
3. Complete a vulnerabilities assessment
4. Complete a security risk review
5. Develop an Incident and Emergency Management Plan
6. Communicate that plan
7. Regularly review that plan
8. Undertake desktop exercises
9. Implement training programs
10. Involve external agencies in walk through
11. Undertake physical security
12. Undertake electronic security
13. Undertake professional security
14. Undertake organisational security

---

**What do you need to do?**

There are a number of key things that should be done when developing an emergency management strategy in order to safeguard your organisation against incidents:

1. Establish an Emergency Planning Committee at each location;
2. Engage professional staff/consultants to undertake the following:
   - establish a threat assessment;
   - determine vulnerabilities;
   - undertake a security risk review; and
   - compile an emergency management plan, including response, communication and escalation protocols.
3. Communicate the plan for your facility to key stakeholders, including major retailers, centre staff, and on-site service providers, such as security and cleaning staff;
4. Inform external stakeholders about the plan and its contents, including the police, local councils, and fire brigades;
5. Identify the resources needed and train staff to implement the plan and ensure it remains relevant and effective;
6. Instigate a regular review process for the emergency management plan;
7. Instigate an audit and compliance program.

The Icons and Public Gatherings (Mass Gatherings) Infrastructure Assurance Advisory Group is currently developing a tool kit for mitigating the risk of emergencies arising in mass gathering locations, which will be available later next year.

---

**Are you prepared?**

- Have you identified the credible security threats facing your organisation?
- Do you have an Emergency Management Program?
- Does your Emergency Management Program address the risks posed by your environment and activities?
- Do you have the equipment, supplies, and support to respond effectively?
- Do you regularly review the physical and electronic security within your facilities?
- Do you have working relationships with government representatives and emergency services personnel, particularly the local police command?
- Have you co-ordinated your emergency response plans with the emergency services?
- Have you communicated your plan to all stakeholders?
- Have you provided staff training?
- Do you have mutual support arrangements with others in your sector?
- Would your venue’s emergency response be effective?
- Do you regularly test your plans?
- Have you established agreed protocols for the recovery of your venue?

If your organisation cannot answer yes to each of these questions, you may not be prepared for an emergency.

This brochure outlines key considerations that will need to be addressed to allow the owners, managers, and occupiers of mass gathering locations to protect their facilities, employees and visitors.

Emergency management allows businesses to prepare for almost any eventuality in the interests of good corporate governance and maintaining control of the premises.

As such, it is an integral part of an organisation’s business continuity processes.

Emergency management should consider all hazards, not just terrorism-related incidents. This means that a plan can be applied to any of the following:

- Fire
- Bomb threats or explosions
- Flooding
- Gas leaks
- Power outages and losses of services
- Structural collapse
- Armed intrusion
- Demonstrations
- Earthquakes
- Airborne contaminants
- Fatalities/suicide
- Public brawling/unrest
- Lost child/child abduction

While some basic steps to safeguard against emergency incidents are outlined opposite, readers would also be advised to consider the information contained in the sources identified at the end of this document.

---

**Incident and Emergency Management**

Step 1: Establish an Emergency Planning Committee
Step 2: Complete a threat assessment
Step 3: Complete a vulnerabilities assessment
Step 4: Complete a security risk review
Step 5: Develop an Incident and Emergency Management Plan
Step 6: Communicate that plan
Step 7: Regularly review that plan
Step 8: Undertake desktop exercises
Step 9: Implement training programs
Step 10: Involve external agencies in walk through

---

**Step 1** Document specifications

**Step 2** Audit existing equipment

**Step 3** Identify decision makers

**Step 4** Lobby for change at all levels

---

**Emergency management should consider all hazards, not just terrorism-related incidents.** This means that a plan can be applied to any of the following:

- Fire
- Bomb threats or explosions
- Flooding
- Gas leaks
- Power outages and losses of services
- Structural collapse
- Armed intrusion
- Demonstrations
- Earthquakes
- Airborne contaminants
- Fatalities/suicide
- Public brawling/unrest
- Lost child/child abduction

While some basic steps to safeguard against emergency incidents are outlined opposite, readers would also be advised to consider the information contained in the sources identified at the end of this document.

---

**External Relations**

1. Complete a vulnerabilities assessment
2. Determine what external influences increase your vulnerability
3. Identify decision makers
4. Lobby for change at all levels

**Professional Security Staff**

1. Communicate organisational expectations
2. Recruit professional staff and undertake a formal induction
3. Develop organisational procedures
4. Develop facility-specific site orders
5. Implement training programs
6. Develop a Security Management Plan

**Electronic Security**

1. Document specifications
2. Communicate expectations and objectives
3. Audit existing equipment
4. Seek professional advice

**Physical Security**

1. Document specifications
2. Communicate expectations and objectives
3. Audit existing equipment
4. Seek professional advice

---

If your organisation cannot answer yes to each of these questions, you may not be prepared for an emergency.

This brochure outlines key considerations that will need to be addressed to allow the owners, managers, and occupiers of mass gathering locations to protect their facilities, employees and visitors.

Emergency management allows businesses to prepare for almost any eventuality in the interests of good corporate governance and maintaining control of the premises.

As such, it is an integral part of an organisation’s business continuity processes.

Emergency management should consider all hazards, not just terrorism-related incidents. This means that a plan can be applied to any of the following:

- Fire
- Bomb threats or explosions
- Flooding
- Gas leaks
- Power outages and losses of services
- Structural collapse
- Armed intrusion
- Demonstrations
- Earthquakes
- Airborne contaminants
- Fatalities/suicide
- Public brawling/unrest
- Lost child/child abduction

While some basic steps to safeguard against emergency incidents are outlined opposite, readers would also be advised to consider the information contained in the sources identified at the end of this document.
This brochure should be considered in light of the briefings given by the Attorney General’s Department and Australian Security Intelligence Organisation, which relate to the following national alert levels (see www.nationalsecurity.gov.au)

Low: No information to suggest a terrorist attack in Australia
Medium: Medium risk of a terrorist attack in Australia
High: High risk of a terrorist attack in Australia
Extreme: A terrorist attack is imminent or has occurred

Publications

AS 3745 – 2002 – Emergency control organisation and procedures for buildings, structures, and workplaces – Standards Australia
AS 4360 – 2004 – Risk management – Standards Australia
Security planning and counter-terrorism coordination in Queensland; Considerations for owners and operators of mass gathering infrastructure – Queensland Government
Emergency Management in Venues – Emergency Management Australia
Information Pack for Places of Gatherings – Victorian Police Force

Some Useful Websites

Attorney-General’s Department
http://www.nationalsecurity.gov.au
http://www.tisn.gov.au
Emergency Management Australia
http://www.ema.gov.au
emergencyNSW – SydneyAlert
NSW Police Service Secure Automated Notification System
https://www.sans.police.nsw.gov.au
Project Griffin
http://www.cityoflondon.police.uk/countering-terrorism/terrorism-griffin.html
US Department of Homeland Security Standards Database
http://www.hsds.us/
NYPD Shield

Property Council Contacts

Peter Verwer, CEO  Tel: 02 9033 1926 Email: pverwer@propertyoz.com.au
Paul Waterhouse  Tel: 02 9033 1956 Email: pwaterhouse@nsw.propertyoz.com.au

Glossary

Mass gatherings – any location where large numbers of people come together. This can include shopping centres, sporting venues, hotels, and entertainment precincts.

Threat assessment – identifies and evaluates each type of threat (both natural and man made) to the asset, including the context in which that threat operates (i.e. “who/what/when/where/why”).

Vulnerability assessment – measures the potential impact from specific threat scenarios based on existing conditions, including possible damage to assets and injury to persons. It provides a baseline for determining the potential benefits from improvements to existing processes (i.e. “what if”).

Security risk review – incorporates both the threat and vulnerability assessments with an evaluation of existing programs, resources and security measures. It ranks existing risks and makes recommendations to reduce medium and high risks, as far as is reasonably and practically possible through the use of a Risk Matrix and preventative strategy.

Emergency Management Plan – a “crash kit” which outlines pre-planned responses to specific threats and includes media handling procedures, staff contact lists, stakeholders contact lists and critical and essential services shutdown plans as well as detailed ‘structural’, ‘HVAC’, and ‘tactical fire’ plans.